



Dział zamówień publicznych

Gdańsk, data 07.01.2020 r.

dot. postępowania o udzielenie zamówienia prowadzone w trybie przetargu nieograniczonego na dostawę wielostanowiskowej licencji oraz trzyletniej subskrypcji na oprogramowanie antywirusowe wraz z wdrożeniem dla Politechniki Gdańskiej ZP/320/055/D/19

Zamawiający na podstawie art. 38 ust. 2 i ust. 4 ustawy Prawo zamówień publicznych (t.j. Dz. U. z 2019 r., poz. 1843 z późn. zm.) informuje, iż do Zamawiającego wpłynęło pytanie dotyczące treści Specyfikacji Istotnych Warunków Zamówienia (SIWZ), na które Zamawiający udziela odpowiedzi oraz dokonuje zmiany zapisów Siwz.

Pytanie 1:

"ochrona/blokowanie napędów : możliwość kontroli i ograniczenia dostępu do wybranych napędów i portów komputera."

Czy zamawiający dopuszcza możliwość kontroli i ograniczania dostępu do wybranych kategorii urządzeń w tym napędów optycznych, pamięci masowych, urządzeń masowych urządzeń dowolnego typu?

Odpowiedź:

Tak, Zamawiający dopuszcza taką możliwość.

Pytanie 2:

"Możliwość stworzenia hierarchii serwerów i definiowania nadrzędności/podrzędności serwera."

Czy zamawiający dopuszcza wykorzystanie jednego serwera centralnego zarządzania mogącego obsłużyć do 250 tys. hostów jednocześnie z możliwością wykorzystania dodatkowych serwerów pośredniczących z funkcjonalnością cache'owania pobieranych modułów aplikacji, w tym baz sygnatur wirusów oraz instalatorów aplikacji ?

Odpowiedź:

Tak, zamawiający dopuszcza Wykorzystanie jednego serwera centralnego (w praktyce po jednym serwerze głównym dla każdego pliku licencji).

Pytanie 3:

"Możliwość uruchomienia serwera administracyjnego na systemie Windows, brak konieczności instalacji dodatkowych serwerów takich jak ISS czy Apache."

Czy zamawiający dopuszcza wykorzystanie serwera Apache Tomcat jako składnika instalowanego automatycznie bez konieczności dodatkowej konfiguracji ze strony klienta, ewentualnie możliwość wykorzystania funkcji RMM jako funkcji zdalnego monitorowania i zarządzania (Remote Monitoring and Management, RMM). Jest to proces nadzorowania i kontrolowania systemów oprogramowania przy użyciu lokalnie zainstalowanego agenta, do którego ma dostęp dostawca usługi zarządzania ?

Odpowiedź:

Tak, zamawiający dopuszcza instalację modułów firm trzecich o ile proces ich instalacji jest w pełni zautomatyzowany i nie wymaga od Zamawiającego zakupu dodatkowych licencji.

Pytanie 4:

Zamawiający wymaga by klucz produktu wystawiony na nazwę i adres zamawiającego, rozbity był na kilka plików.

Czy zamawiający dopuszcza zarządzanie tymi kluczami spod jednej konsoli w Cloud?

Odpowiedź:

Tak, zamawiający dopuszcza takie rozwiązanie, o ile będzie możliwość hierarchicznego zarządzania uprawnieniami do poszczególnych kluczy za pomocą zdefiniowanych użytkowników.

Pytanie 5:

Zamawiający wskazuje - możliwość edycji monitorowanych portów .

Czy zamawiający dopuszcza rozwiązanie które będzie mogło monitorować porty automatycznie bez ich edycji.

Odpowiedź:

Tak, zamawiający uzna takie rozwiązanie za równoważne.

Pytanie 6:

Zamawiający wskazuje - **ochrona sieci** : możliwość ukrywania portów dla wybranych sieci, możliwość definiowania stref zaufanych, możliwość definiowania reguł dla portów, protokołów, aplikacji, możliwość eksportu i importu ustawień zapory, możliwość przełączania zapory w tryb uczenia, możliwość podglądu otwartych portów, zestawionych połączeń i ruchu sieciowego

Czy zamawiający dopuszcza rozwiązanie które nie posiada możliwości przełączenia zapory w tryb uczenia lecz pozwala na ręcznie definiowanie reguł oraz dodatkowo posiada funkcjonalności takie jak:

- możliwość ukrywania portów dla wybranych sieci
- blokowanie skanowania portów
- monitorowanie połączeń WIFI
- możliwość definiowania stref zaufanych
- możliwość definiowania reguł dla portów, protokołów, aplikacji

Bez poniższych funkcjonalności ochrony sieci :

- możliwość eksportu i importu ustawień zapory,
- możliwość podglądu otwartych portów, zestawionych połączeń i ruchu sieciowego

Odpowiedź:

Tak, zamawiający uzna takie rozwiązanie za równoważne pod warunkiem zapewnienia innej funkcjonalności automatycznego ustawienia identycznych polityk bezpieczeństwa wdrożonych na stacji roboczej A, dla stacji roboczej B, C, D itd..

Pytanie 7:

Zamawiający wskazuje - możliwość ochrony rejestru systemowego
Czy zamawiający dopuszcza rezygnację z tej funkcji?

Odpowiedź:

Tak, Zamawiający dopuści rezygnację z takiej funkcji jeśli zaoferowany produkt posiada funkcjonalność ochrony przed modyfikacją składników systemu takich jak usługi i programy automatycznie uruchamiane wraz ze startem systemu.

Pytanie 8:

Zamawiający wskazuje - mechanizm sygnalizowania infekcji, prób włamań, błędów stacji roboczych oraz raportowania ich za pomocą wiadomości e-mail
Czy zamawiający dopuszcza rozwiązanie w którym próby włamań będą powiadomieniem z zapory sieciowej?

Odpowiedź:

Opisany mechanizm jest narzędziem administratora, nie użytkownika końcowego - źródło może być dowolne, ale alert na życzenie musi dotrzeć do administratora za pomocą usługi poczty elektronicznej.

Pytanie 9:

Zamawiający wskazuje - mechanizm zarządzania licencjami z możliwością sumowania liczby użytych licencji
Czy zamawiający dopuszcza rozwiązanie w którym zarządzanie i sumowanie licencji odbywa się per serwer?

Odpowiedź:

Tak, dopuszcza się takie rozwiązanie.

Pytanie 10:

Zamawiający wskazuje - możliwość stworzenia hierarchii serwerów i definiowania nadrzędności/ podrzędności serwera
Czy zamawiający dopuszcza rozwiązanie w którym hierarchia serwerów będzie dostępna w konsoli zarządzającej opartej o chmurę?

Odpowiedź:

Zamawiający dopuszcza takie rozwiązanie, o ile infrastruktura chmury będzie znajdować się na serwerach Zamawiającego.

Pytanie 11:

Zamawiający wskazuje - przechowywanie danych w relacyjnej bazie danych
Czy zamawiający dopuszcza użycie bazy danych MongoDB?

Odpowiedź:

Tak, Zamawiający dopuszcza inne rodzaje baz danych.

Pytanie 12:

Zamawiający wskazuje - możliwość uruchomienia serwera administracyjnego na systemie Windows, brak konieczności instalacji dodatkowych serwerów takich jak ISS czy Apache
Czy zamawiający dopuszcza rozwiązanie w którym serwer administracyjny jest maszyną wirtualną z własnym systemem operacyjnym?

Odpowiedź:

Tak, Zamawiający dopuszcza takie rozwiązanie tylko w przypadku maszyn zgodnych z używaną przez Zamawiającego infrastrukturą Vcenter firmy Vmware.

Pytanie 13:

W Załączniku nr 4 do Siwz postępowania ZP/320/055/D/19 „SPECYFIKACJA TECHNICZNA PAKIETU ANTYWIRUSOWEGO” jako przedmiot zamówienia definiują Państwo „Wdrożenie i migracja” jako:

- w przypadku zaoferowania produktu innego niż obecnie używany przez Zamawiającego, Wykonawca zobowiązany jest do pomocy we wdrożeniu i migracji z obecnie używanego oprogramowania Kaspersky Business Space Security do oprogramowania zaoferowanego. Pomoc taka obejmuje zdalne usunięcie oprogramowania dotychczas używanego i konfigurację oraz wdrożenie paczek instalacyjnych zaoferowanego produktu na stacjach roboczych w środowisku bez domeny Windows oraz szkolenia dla administratorów w zakresie konfiguracji i instalacji produktu antywirusowego, serwera i konsoli zarządzającej. Termin wykonania wdrożenia i migracji do dnia 29 stycznia 2020”

Prosimy o doprecyzowanie tego punktu.

- 1) Z ilu stacji roboczych należy usunąć aktualnie wykorzystywane oprogramowanie i czy Zamawiający zapewni do nich zdalny dostęp umożliwiający odinstalowanie oprogramowania w okresie od podpisania umowy do terminu wykonania wdrożenia i migracji, to jest do 29 stycznia 2020.
- 2) Na ilu stacjach roboczych należy zainstalować nowe oprogramowanie i czy Zamawiający zapewni do nich zdalny dostęp umożliwiający instalację oprogramowania w okresie od podpisania umowy do terminu wykonania wdrożenia i migracji, to jest do 29 stycznia 2020.
- 3) Ilu administratorów Zamawiający chce przeszkolić?
- 4) Czy organizacja szkolenia ma uwzględniać wynajem Sali i zapewnienie niezbędnej infrastruktury?

Odpowiedź:

- 1) i 2) Zamawiający uzna, że w/w warunki zostały spełnione jeśli Wykonawca zapewni pomoc wdrożeniową przy tworzeniu nowych paczek instalacyjnych, które w sposób nienadzorowany umożliwią uprzednią deinstalację oprogramowania Kaspersky oraz instalację zaoferowanego oprogramowania w środowisku bez domeny Windows. Instalacja taka może być wywołana ręcznie przez użytkownika końcowego np. przez uruchomienie pliku wykonywalnego, skryptu itp. Zamawiający nie udostępnia zdalnego dostępu do maszyn klienckich w inny sposób niż poprzez mechanizm serwera i agenta usług Kaspersky. Wdrożenie i migracja zostanie przez Zamawiającego uznana, za zakończoną jeśli Wykonawca wykona instalację serwera (maksymalnie 9 serwerów) i

konsoli zarządzającej, ustalone zostaną polityki bezpieczeństwa i zostanie dostarczony mechanizm deinstalacji starych i instalacji nowych produktów, nie jest wymagane, aby w terminie realizacji przedmiotu zamówienia, wszystkie końcówki Zamawiającego posiadały nowo zainstalowane oprogramowanie, dlatego ich ilość nie jest istotna.

- 3) Zespół do 30 osób.
- 4) Zamawiający dysponuje odpowiednią infrastrukturą do przeprowadzenia szkoleń - salę, projektor z ekranem, szybkie połączenie internetowe.

Jednocześnie Zamawiający zmienia termin realizacji przedmiotu umowy z 14 dni kalendarzowych na 10 dni kalendarzowych. W związku z tym zmianie ulega zapis w:

- 1) Rozdziale IV Siwz

Jest: Termin realizacji zamówienia: do 14 dni kalendarzowych od dnia zawarcia umowy lub do wyczerpania kwoty umowy.

Powinno być: Termin realizacji zamówienia: do 10 dni od dnia zawarcia umowy.

- 2) Załączniku nr 5 do Siwz, par. 3 ust. 1

Jest: Wykonawca zobowiązuje się zrealizować dostawę przedmiotu umowy w terminie 14 dni licząc od dnia podpisania Umowy.

Powinno być: Wykonawca zobowiązuje się zrealizować dostawę przedmiotu umowy w terminie 10 dni licząc od dnia podpisania Umowy.

- 3) Załączniku nr 4 do Siwz w pozycji „Wdrożenie i migracja” zmienia się zapis:

Jest:.... Termin wykonania wdrożenia i migracji do dnia 29 stycznia 2020....

Powinno być:.... Termin wykonania wdrożenia i migracji do 10 dni od dnia podpisania umowy....

Pytanie 14:

Czy zamawiający dopuszcza możliwość częściowego wdrożenia do tej daty (połowa stacji), a finalna migracja oprogramowania zakończy się do końca lutego 2020?

Odpowiedź:

Termin wykonania wdrożenia zgodnie z projektem umowy tj. 10 dni od dnia podpisania umowy.

Ponadto, Zamawiający uzna, że warunki wdrożenia zostały spełnione jeśli Wykonawca zapewni pomoc wdrożeniową przy tworzeniu nowych paczek instalacyjnych, które w sposób nienadzorowany umożliwią uprzednią deinstalację oprogramowania Kaspersky oraz instalację zaoferowanego oprogramowania w środowisku bez domeny Windows. Instalacja taka może być wywołana ręcznie przez użytkownika końcowego np. przez uruchomienie pliku wykonywalnego, skryptu itp. Zamawiający nie udostępnia zdalnego dostępu do maszyn klienckich w inny sposób niż poprzez mechanizm serwera i agenta usług Kaspersky. Wdrożenie i migracja zostanie przez Zamawiającego uznana, za zakończoną jeśli Wykonawca wykona instalację serwera (maksymalnie 9 serwerów) i konsoli zarządzającej, ustalone zostaną polityki bezpieczeństwa i zostanie dostarczony mechanizm deinstalacji starych i instalacji nowych produktów, nie jest wymagane aby wszystkie końcówki Zamawiającego posiadały nowo zainstalowane oprogramowanie.

Pytanie 15:

możliwość ukrycia ikony programu przed użytkownikiem – czy Zamawiający dopuszcza rozwiązanie osiągające taką funkcjonalność jednak realizowaną nie bezpośrednio z poziomu konsoli zarządzającej?

Odpowiedź:

Zamawiający nie dopuszcza rozwiązań konfigurowalnych wyłącznie na kliencie końcowym. Możliwość ukrycia ikony programu powinna być konfigurowana zdalnie.

Pytanie 16:

Czy Zamawiający dopuści rozwiązanie konfigurowalne ręcznie bez możliwości przełączania zapory w tryb uczenia bez podglądu zestawionych połączeń i ruchu sieciowego?

Odpowiedź:

Tak, Zamawiający dopuści taką funkcjonalność.

Pytanie 17:

Czy dopuszcza się rozwiązanie bez możliwości definicji kilku źródeł aktualizacji o funkcjonalności: "jeśli opcja pobierz z X, jest niedostępne, to pobierz z Y"?

Odpowiedź:

Tak, Zamawiający dopuszcza takie rozwiązanie pod warunkiem, że adres serwera aktualizacji jest tak naprawdę pulą serwerów, a o kolejności ich użycia decyduje mechanizm balansowania.

Pytanie 18:

Czy Zamawiający uzna rozwiązanie bez mechanizmu zarządzania licencjami z możliwością sumowania liczby użytych licencji?

Odpowiedź:

Zamawiający uzna możliwość sumowania liczby użytych licencji jako mechanizm służący do ich zarządzania.

Pytanie 19:

Czy rozwiązanie dostępne w większości w języku polskim i częściowo angielskim (dot. głównie dokumentacji technicznej) jest dla Zamawiającego akceptowalne?

Odpowiedź:

Wymagane jest aby interfejs użytkownika aplikacji klienckiej, pomoc i komunikaty wyświetlane w interakcji z użytkownikiem były w języku polskim. Zamawiający dopuszcza częściowe tłumaczenie (w tym dokumentacji technicznej), warunkowo w okresie przejściowym, przy aktualizacjach do nowych wersji zaoferowanego oprogramowania.

Ponadto Zamawiający zmienia zapis w Załączniku nr 6 do Siwz w pkt 1 ppkt c), który otrzymuje brzmienie: Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego nr ZP/320/055/D/19 na dostawę wielostanowiskowej licencji oraz trzyletniej subskrypcji na oprogramowanie antywirusowe wraz z wdrożeniem dla PG w trybie przetargu nieograniczonego.



**POLITECHNIKA
GDAŃSKA**

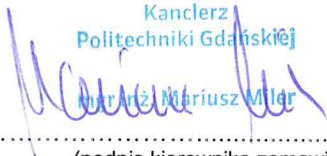
Zamawiający informuje, iż termin składania i otwarcia ofert ulega zmianie.

Zmianie ulegają zapisy w Rozdziale X pkt. 14 oraz w Rozdziale XI pkt. 2 i 4 SIWZ, dotyczące terminu składania i otwarcia ofert.

Zamawiający przedłuża termin składania ofert do dnia 10.01.20 20r. do godz. 10:30.
W związku z wydłużeniem terminu składania ofert Zamawiający ustala termin otwarcia ofert na dzień 10.01.20 20r. na godz. 11:00.

Udzielone odpowiedzi oraz zmiany będą wiążące dla wszystkich Wykonawców, którzy otrzymali SIWZ oraz opublikowane na stronie www.dzp.pg.edu.pl zgodnie z art. 38 ust. 2 i 4 ustawy Pzp.

Udzielone odpowiedzi i zmiany stają się integralną częścią SIWZ

Kanclerz
Politechniki Gdańskiej

.....
(podpis kierownika zamawiającego
lub osoby upoważnionej)